



(Source) Delacroix: Liberty Leading the People

Fallacy of Decentralisation:

*Between A and Z
or Liberating Dream?*

Nat Sakimura,
Chairman, OpenID Foundation
CEO, NAT.Consulting

Common Web3 Narratives

| Web1 was decentralised

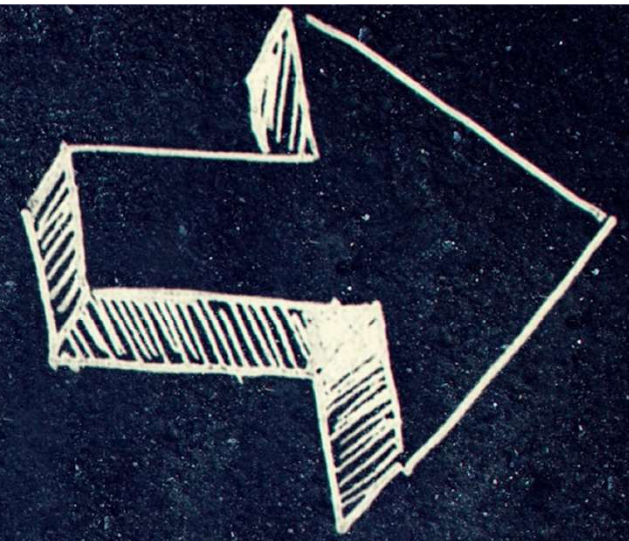
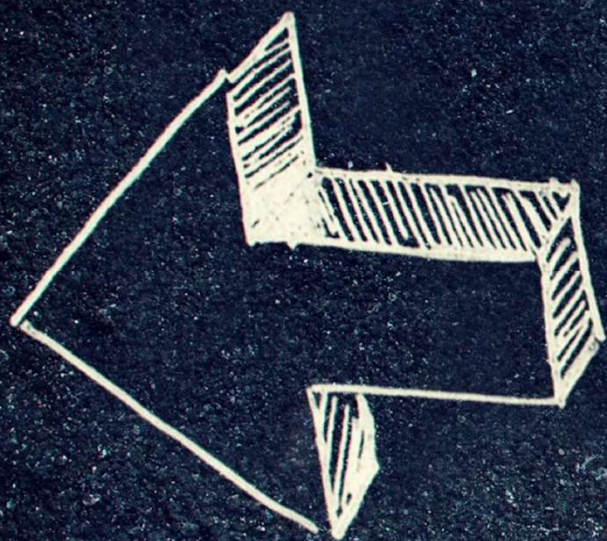
| Web2 is centralised

and dominated by GAFAM/BigTechs.

| Web3 will be decentralised

FACTS

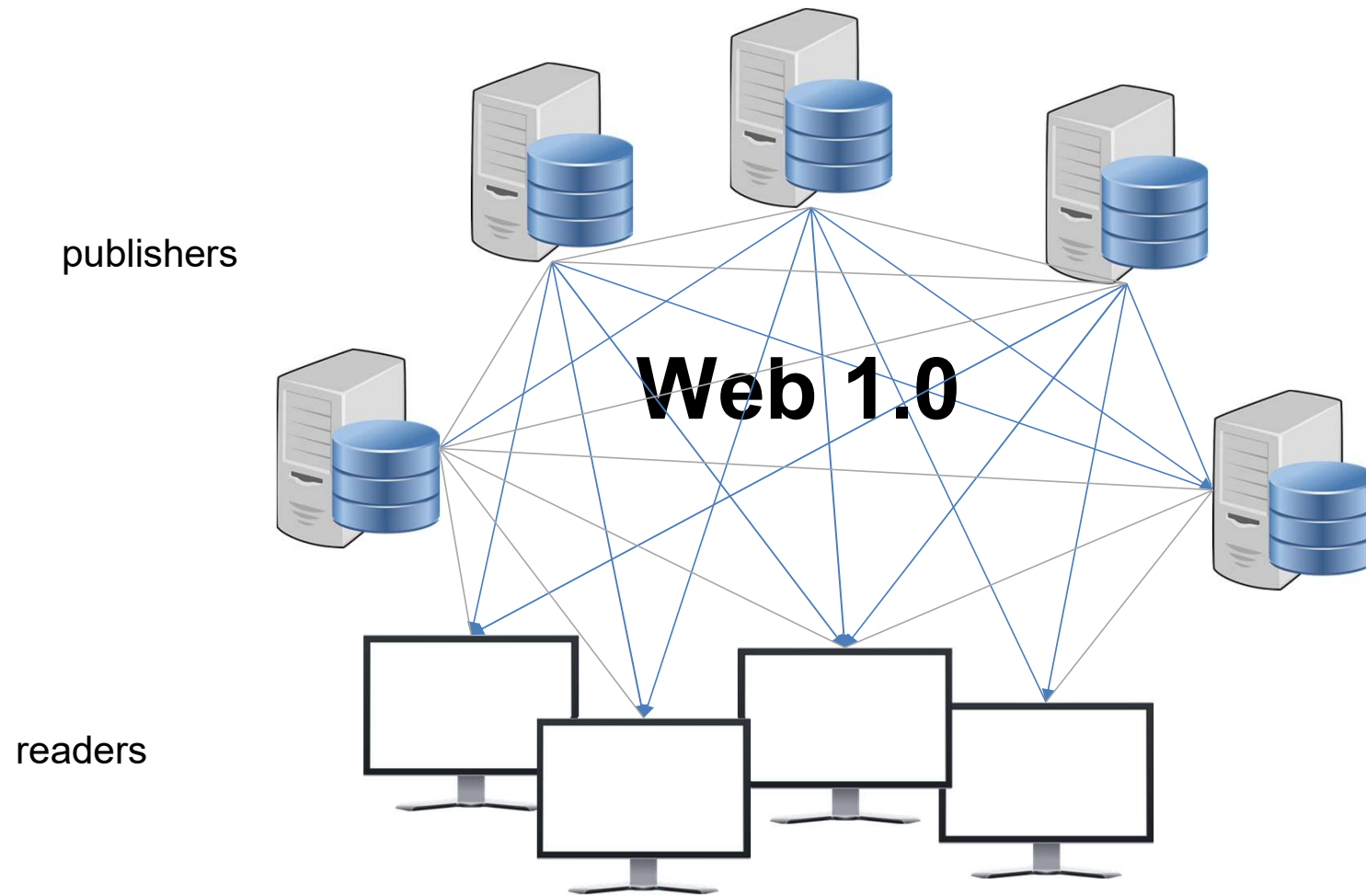
MYTHS





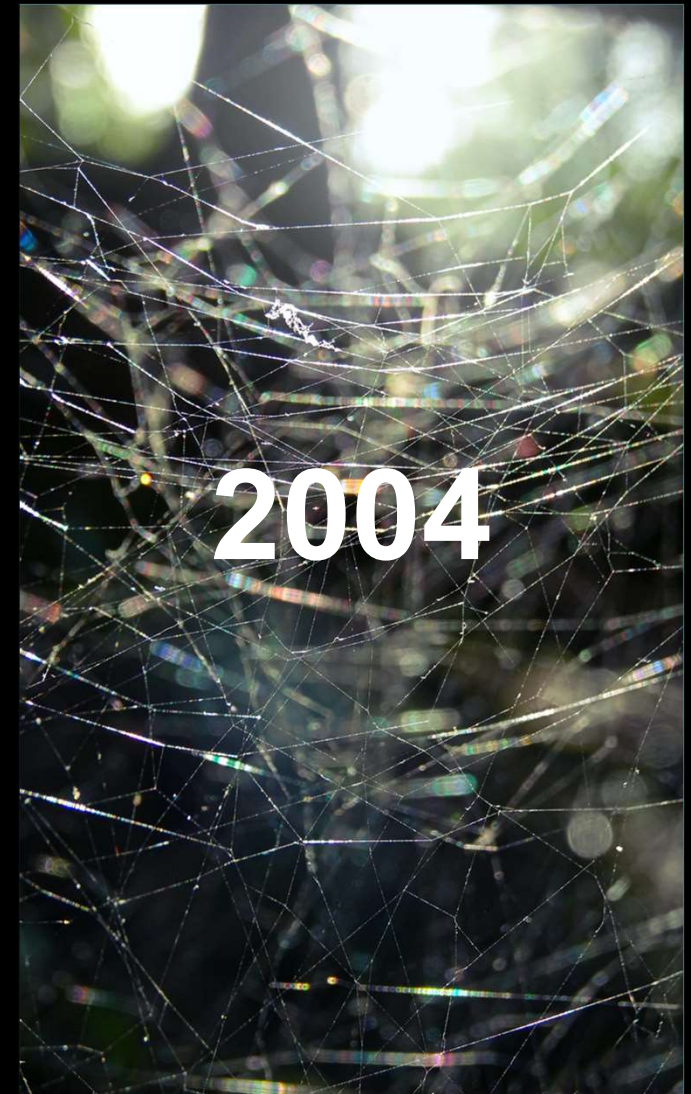
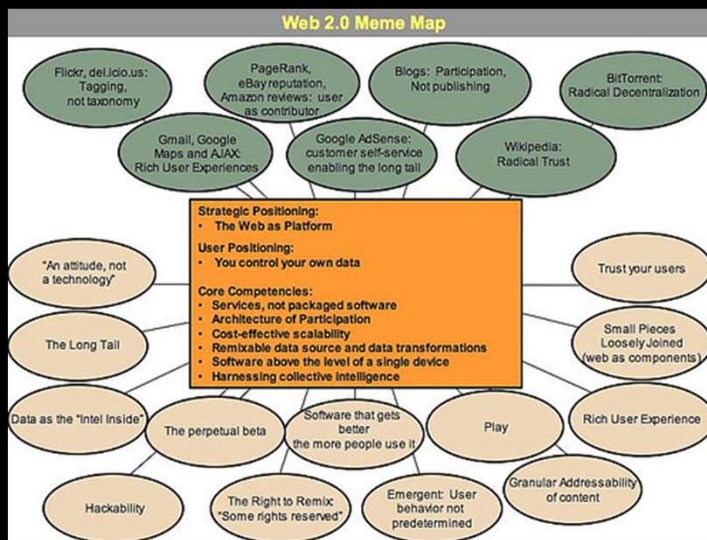
Web 1: Publishing Web Pages

Web1 was about publishing web pages that were linked to other pages. The publishing sites were decentralised all over and were connected by links. Schematics resembled spider webs. Thus, the name “web”.

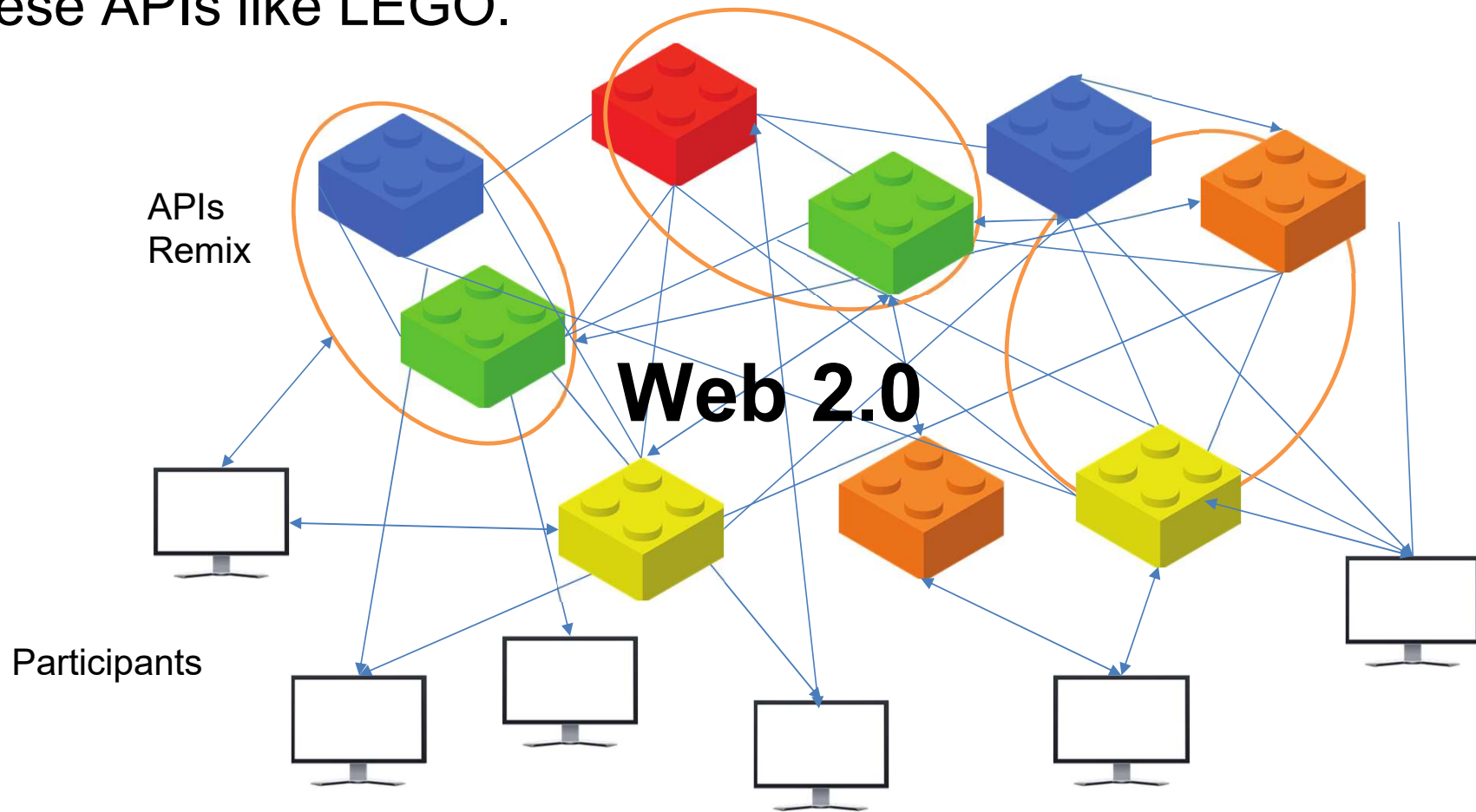


Web 2: API Economy

The API Economy is a key component of Web 2.0, allowing for the decentralization of data and services. This has enabled the development of innovative applications and services that are transforming the way we interact with the world.



instead of monolithic systems, each site provides a function as REST API, and new services quickly emerge by combining these APIs like LEGO.



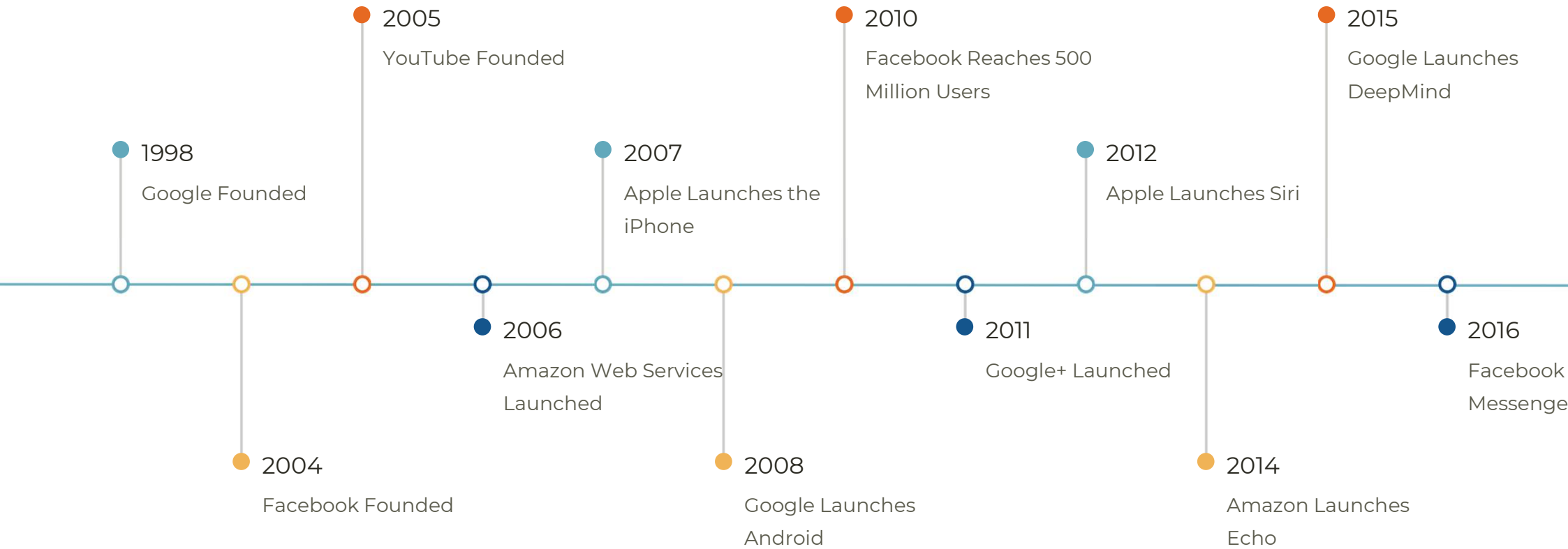


Decentralized to
its extreme



... and GAFA was not dominating.

Growth of GAFAM/BigTechs

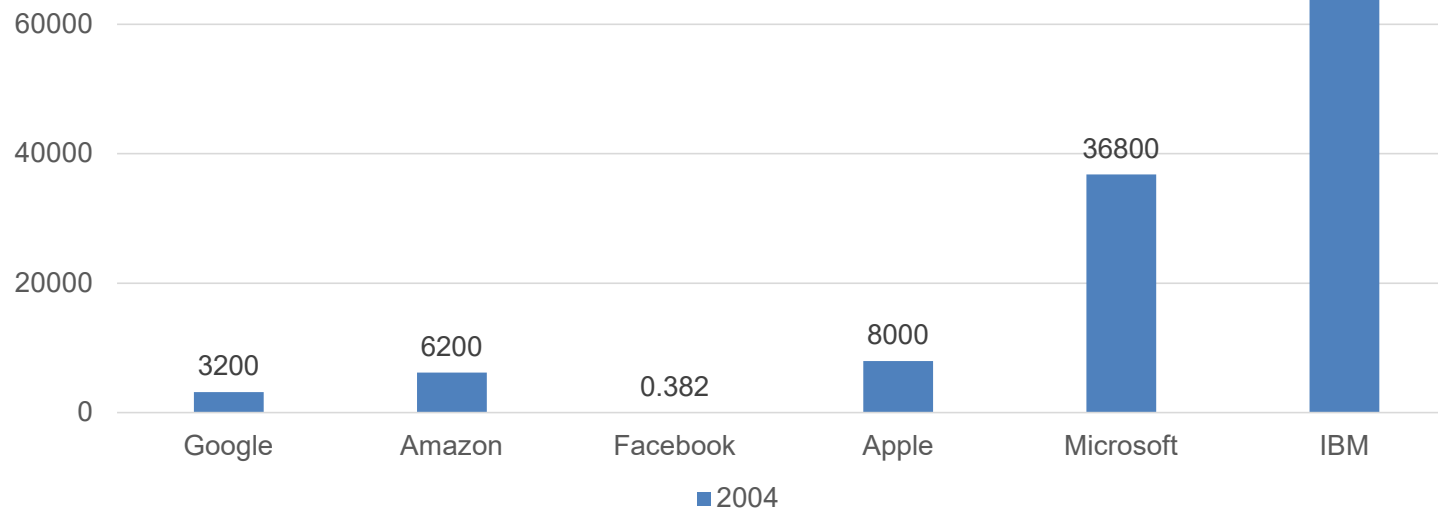


US \$M

2004

120000

GAFA v.s. Microsoft and IBM in 2004





GAFA



IBM
Microsoft

Did we realise decentralization Revolution?

(Source) Jacques-Louis David, Napoleon Crossing the Alps



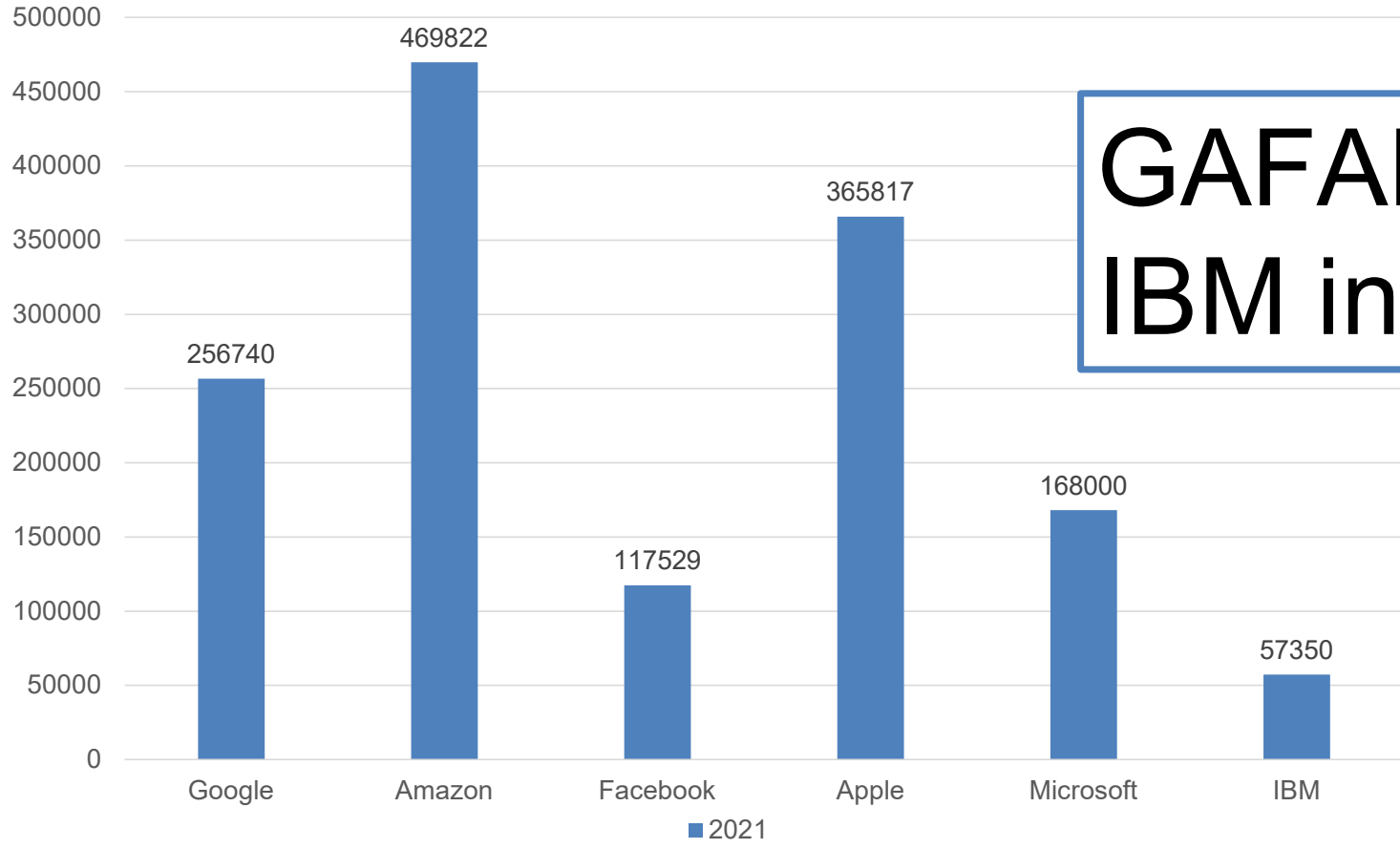
**Clearly, not.
We are now in the
GAFAM dominated
world.**

(Source) Jacques-Louis David: The coronation of Napoleon



US \$M

2021



**GAFAM v.s.
IBM in 2021**

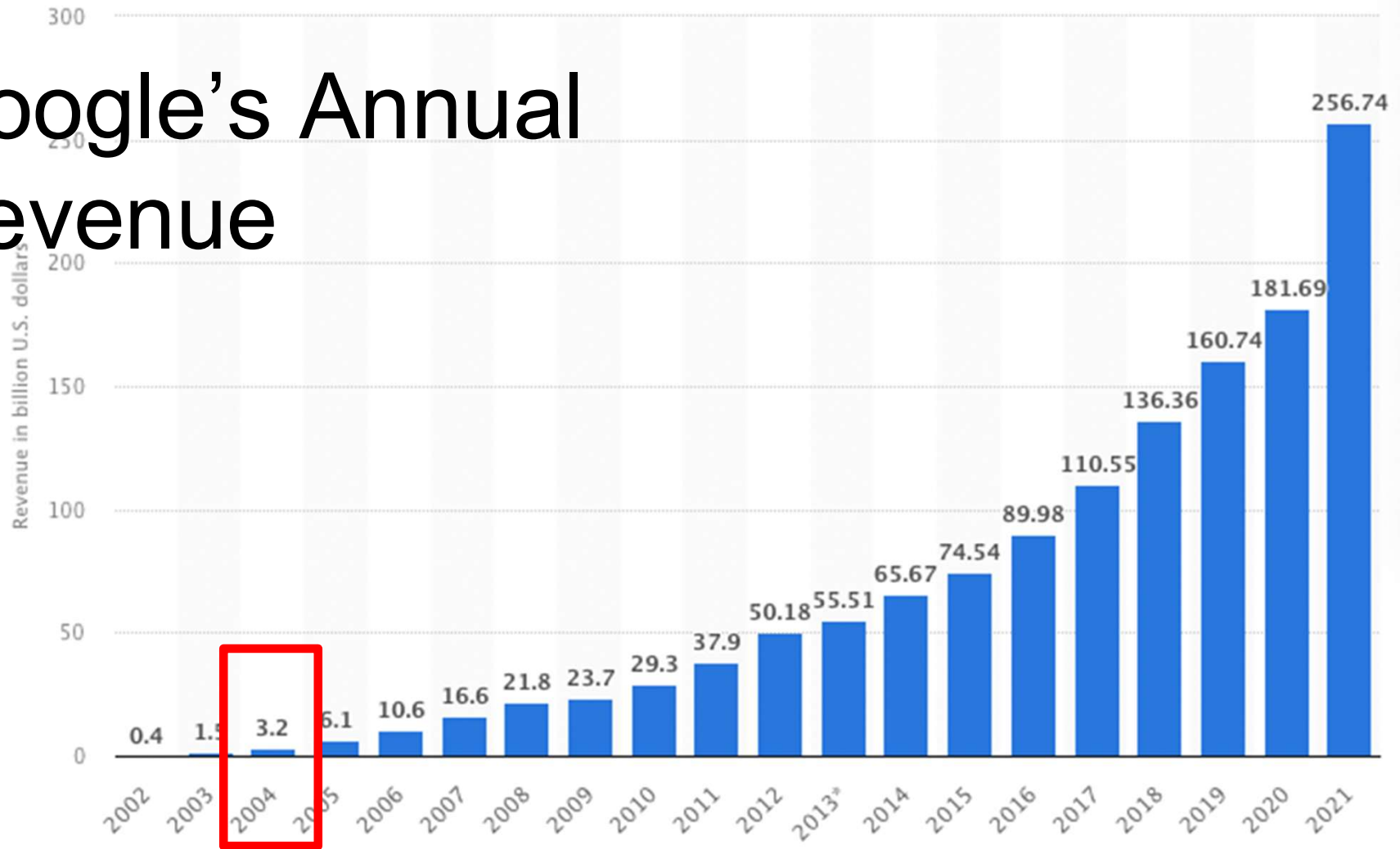


Why?

Why so much concentration despite Web 2.0 being decentralized to the extreme?

Google's Annual Revenue

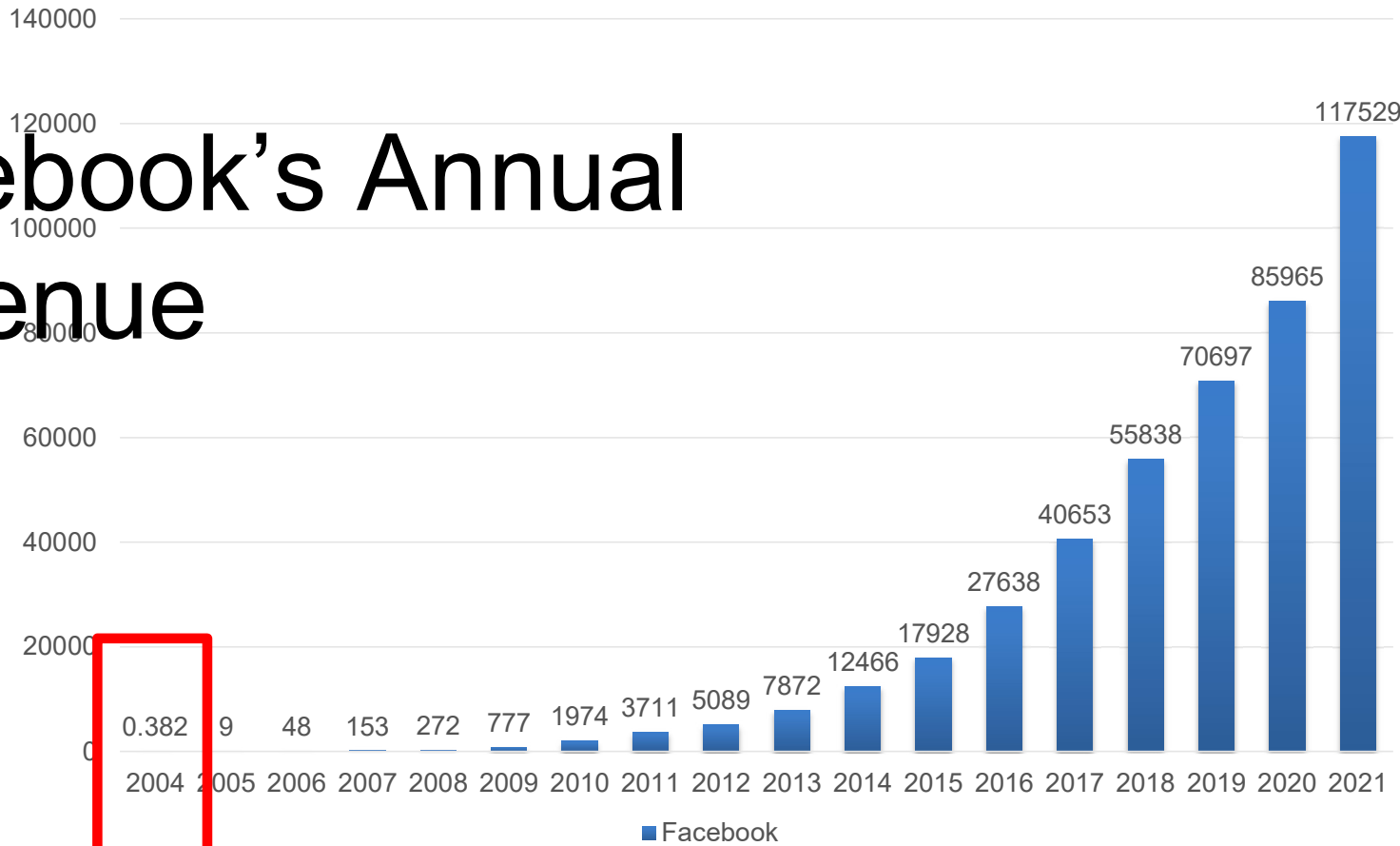
US B\$



US M\$

Facebook

Facebook's Annual Revenue



Increasing
Return and
Free Market
Competition





I N É V I T A B L E



What about WEB 3.0



It still is an information
technology

Exhibits Increasing Return



Gradation of decentralisation

Need to specify what is being “decentralised”

Note that it is not binary between “centralised” and “decentralised”.

Usually, it is in-between.

N = Number of the entities



E.g. Decentralised Ledger

Traditional Ledger: There are N Ledgers for for N entities, i.e. Perfect-Decentralisation

Distributed Ledger: There is only 1 for the entire set of entities, i.e. Perfect-Centralisation

N = Number of entities that writes in Ledgers





What a marketing genius to name a “completely centralised ledger” a “decentralised ledger”!

Degree of “Centralisation” in being “decentralised”

1. 0.34% of addresses own 82.28% of Bitcoin¹
1. LidoDAO has a Gini coefficient of 0.93²
 - a. South Africa has the highest Gini coefficient in the world at 0.63
2. Centralisation of Polygon³:
 - a. 8-key-multi signature for the code base
 - b. There are 4 co-founders
 - c. It takes all the co-founders to collude and another key, potentially a lawyer to drain Polygon

1. <https://bitinfocharts.com/top-100-richest-bitcoin-addresses.html>

2. <https://www.daoitright.xyz/>

3. <https://cryptoslate.com/crypto-investments-fund-founder-says-polygon-is-highly-insecure-centralized/>

Crazy Centralised



Decentralised Identity and Wallet

Instances of IdPs

A Wallet is an IdP. Number of instances will be greater than the number of devices (N) belonging to individuals.

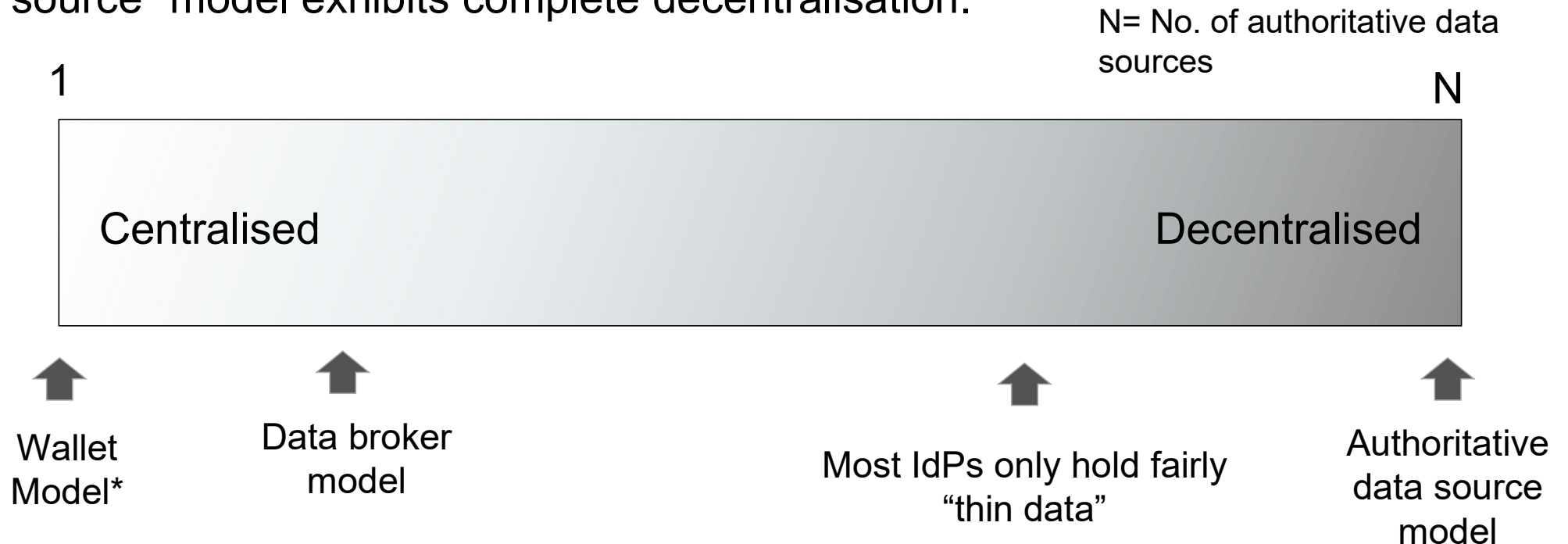
In the context of decentralised identity, this aspect seems to be called out as “decentralised”.

N = Number of devices



Data storage locations

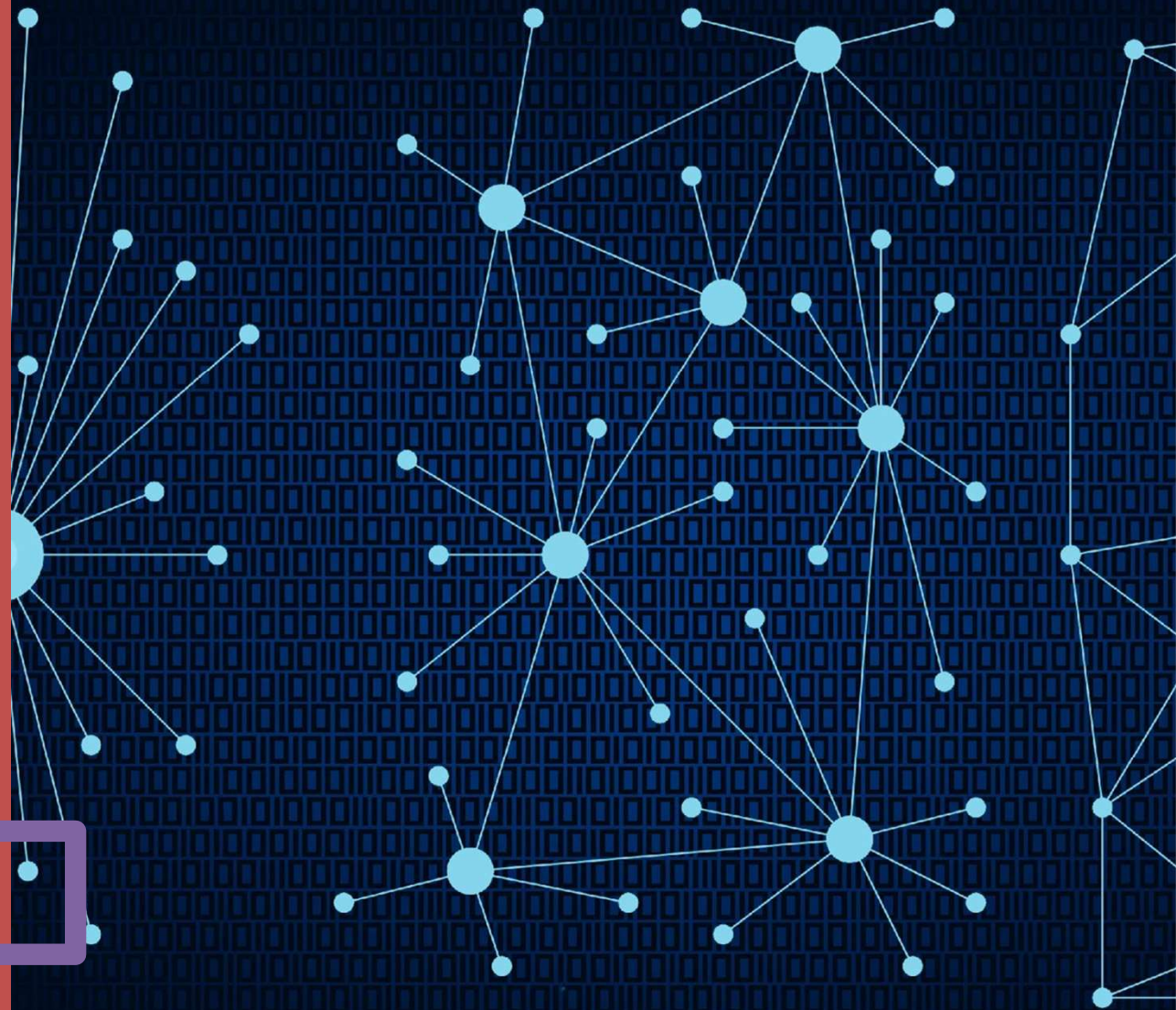
OTH, in the Wallet model, personal data get accumulated in the wallet and thus exhibit hyper-centralisation there, whereas “fetch from authoritative data source” model exhibits complete decentralisation.



* Not only the data but liability also gets accumulated to individuals

VULNERABILITY
DISTRIBUTED LEDGER TECHNOLOGY
HACKING SECURITY
PRIVACY
IDENTITY THEFT
VOLUMETRIC DDOS ATTACK
SIDE CHANNEL ATTACK
RACE CONDITION ATTACK
DISTRIBUTED DENIAL OF SERVICE (DDOS)
NETWORK SECURITY
ADWARE
DATA LEAKAGE
PING OF DEATH ATTACK
FRAGGLE AMPLIFICATION ATTACK
RANSOMWARE
SMURF AMPLIFICATION ATTACK
PASSWORD CRACKING
DDOS ATTACK
DATA MANIPULATION
DECENTRALISED RISK
BACKDOOR ACCESS
DATA TAMPERING
SMURF ATTACK
SPYWARE
INSIDER THREATS
REFLECTION DDOS ATTACK
ICMP FLOOD ATTACK
KEYLOGGER
MAN-IN-THE-MIDDLE ATTACK
CREDENTIAL STUFFING
TROJAN HORSE
REPLAY ATTACK
COOKIE THEFT
DATA SPOOFING
VIRUS
ARP POISONING
SQL INJECTION ATTACK
PHISHING
ZERO-DAY EXPLOIT
WI-FI EAVESDROPPING
ZERO-DAY DDOS ATTACKS
TEARDROP ATTACK
IP SPOOFING
CODE INJECTION ATTACK
CRYPTOJACKING
SYN FLOOD ATTACK
DATA EXFILTRATION
PING FLOOD ATTACK
CROSS-SITE SCRIPTING ATTACK
UDP FLOOD ATTACK
BOTNET
MALWARE
FIREWALL
APPLICATION LAYER DDOS ATTACK
ROOTKIT
DENIAL OF SERVICE ATTACK
SOCIAL ENGINEERING ATTACK
BRUTE FORCE ATTACK
AMPLIFICATION DDOS ATTACK
BLOCKCHAIN
EXPLOIT
DATA INTEGRITY
DISTRIBUTED REFLECTION DENIAL OF SERVICE (DRDOS)
BUFFER OVERFLOW ATTACK
LOGIC BOMB ATTACK
ENCRYPTION
DATA BREACH
THREAT
CRYPTOCURRENCY
SMART CONTRACTS
DISTRIBUTED DENIAL OF SERVICE AS A SERVICE (DDOSAAS)
DISTRIBUTED DENIAL OF SERVICE AS A SERVICE (DDOSAAS)
MALICIOUS CODE

In Web2,
there are 100s
of thousands
of IdPs.



ALIZED

DECENTRALIZED

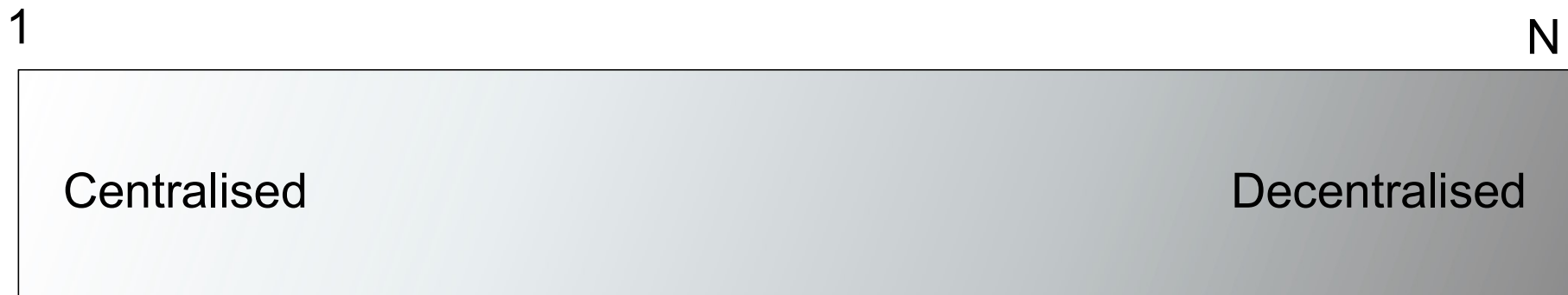
D

Providers of IdPs

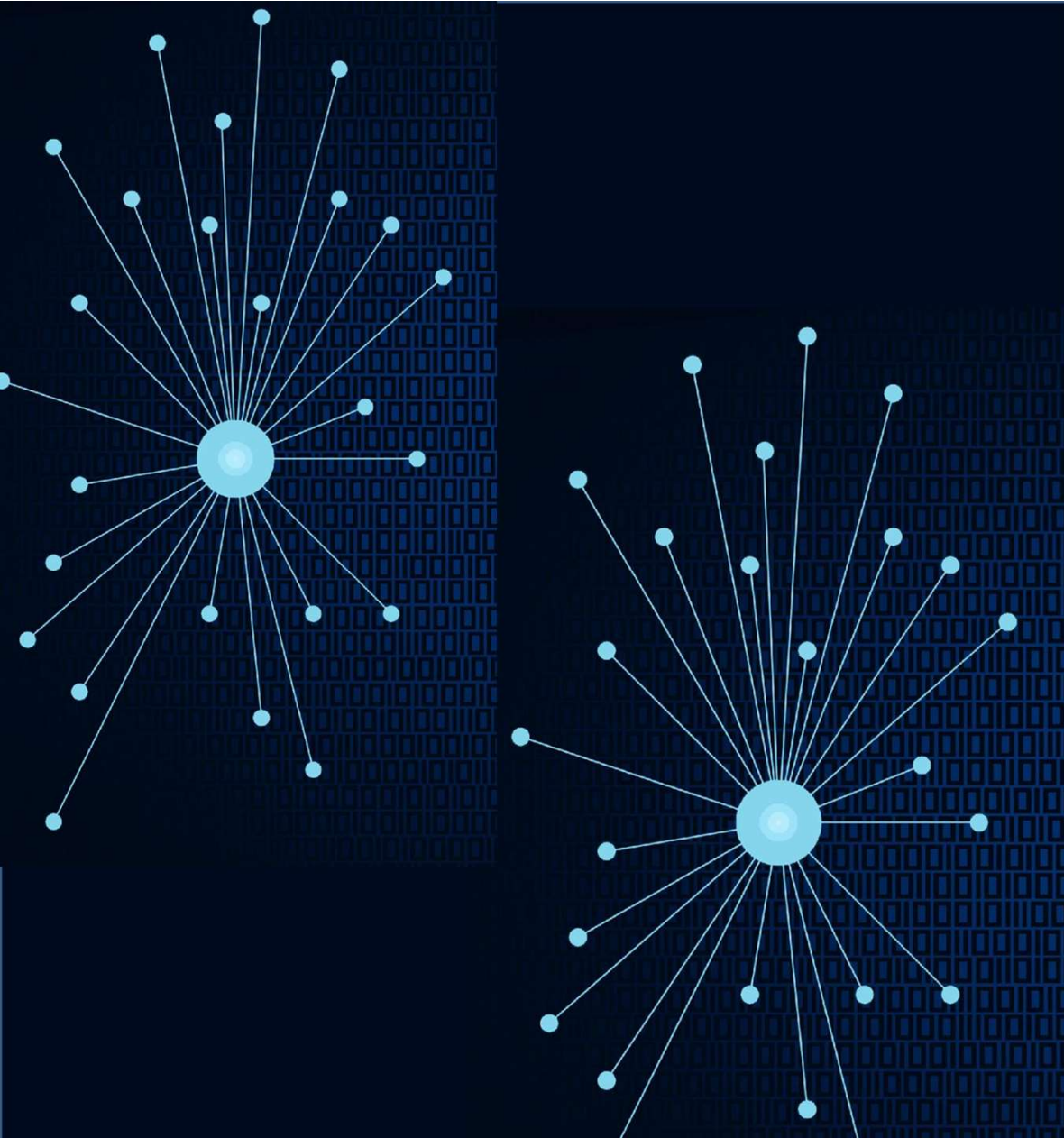
There are over 100K Web 2.0 IdP Providers.

This is very centralised compared to 7.9B (world population) but ...

N = No. of Individuals



↑
IdP
Model



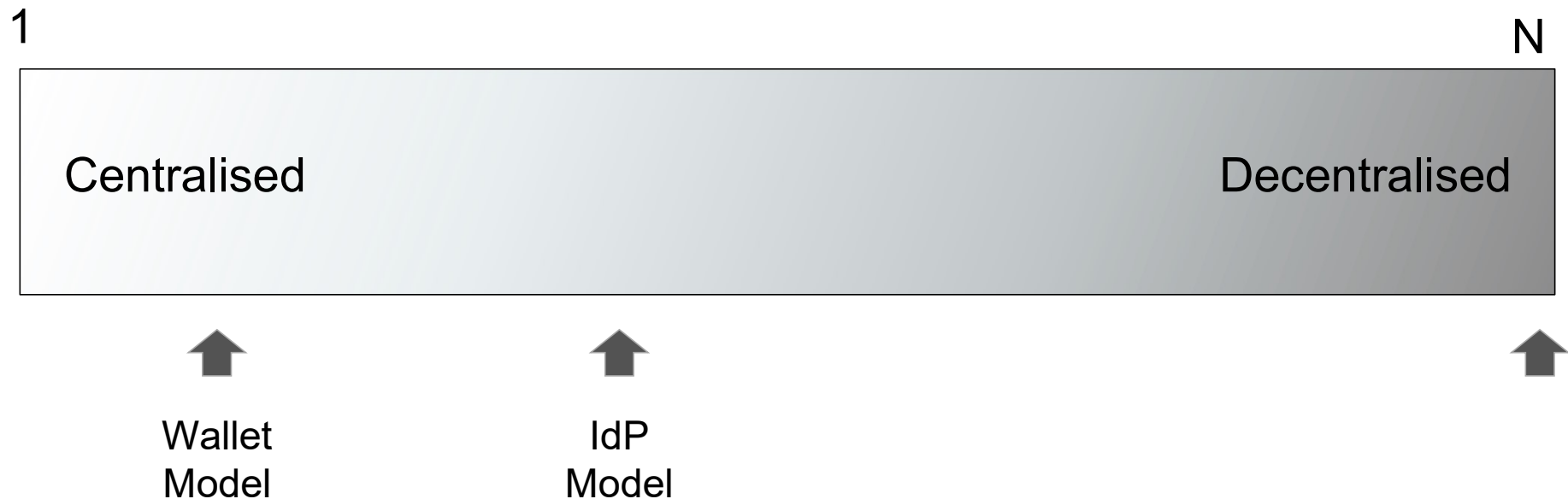
but in wallet
model ...



Providers of IdPs

In the Wallet model, number of wallet providers likely to become significantly smaller than that.

N = No. of individuals



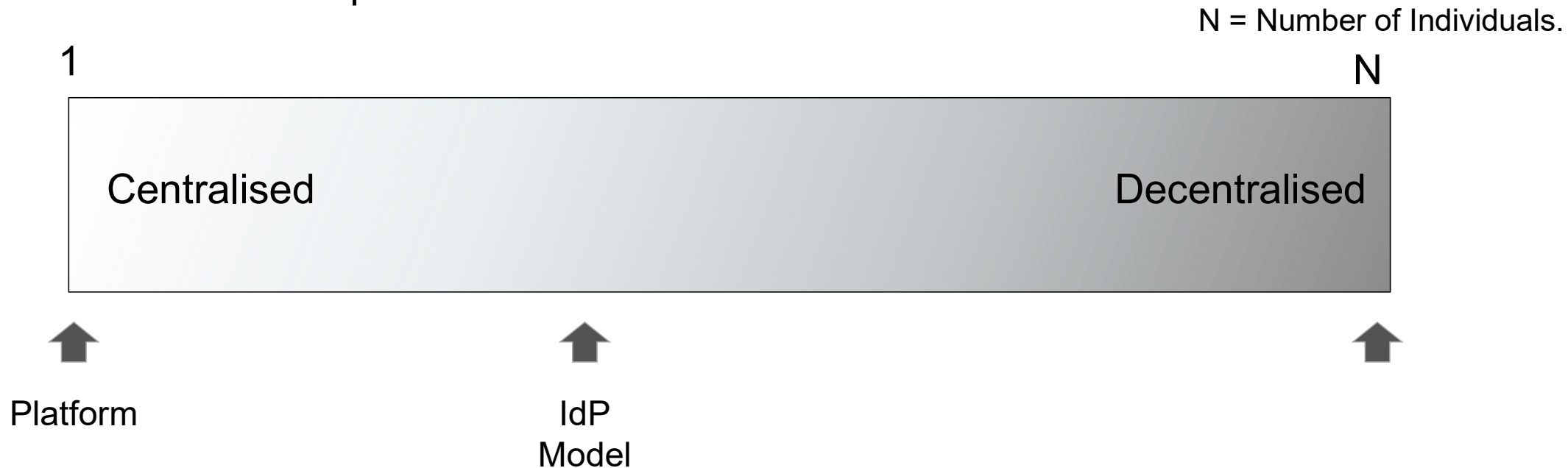


**All wallets are equal but
some are more equal
than others**

(Source) Adopted from the speech of Napoleon in George Orwell's Animal Farm.

Providers of IdP

In the end, it will be centralised to Platform wallet (Apple Wallet, Google Wallet) OR result in OS mediated wallet selection model and it will be centralised to the platforms.



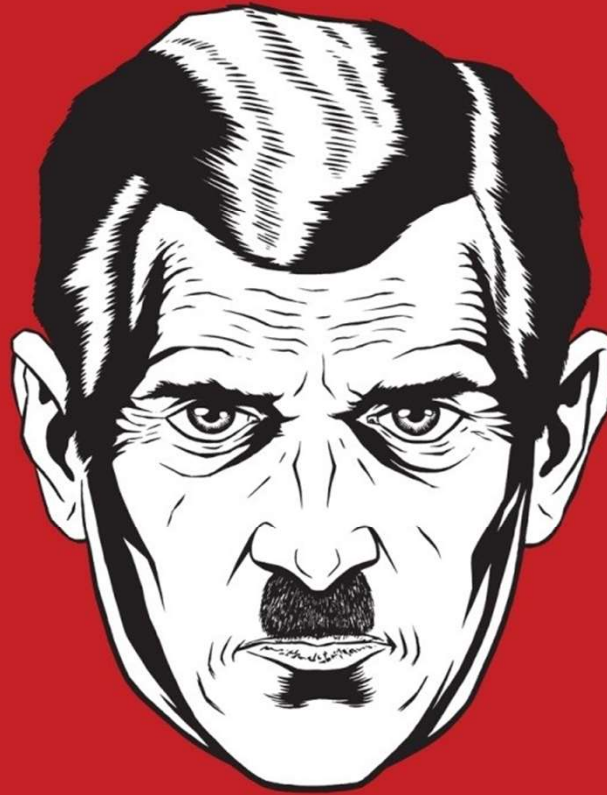
**There could be policy
intervention**



Independent
App Store

Moreover...

**How can you believe the
code that runs on your
phone?**



**BIG BROTHER IS
WATCHING YOU**

(Source) George Orwell: 1984

**Decentralized *adv.* We run our code
on your machine at your own risk.**

(Source) Devil's Dictionary of Linguistic Dark Patterns

Fallacy of Decentralisation

A dark, empty hallway with a single light source from an open doorway at the end, casting a beam of light on the floor.

Is there no light?

WEB 3.0

A digital tunnel with glowing blue and red lines, creating a sense of depth and movement. The text 'WEB 3.0' is prominently displayed in the center, rendered in a glowing, pixelated font. The background is a complex network of lines and nodes, suggesting a data-driven environment.

Not between

A-----
-----Z

but found in

Cypherpunk's
Idealistic
Dream



Innovation



trust in the

running code

A black and white photograph of a dark, narrow tunnel. At the far end of the tunnel, a bright light source, possibly an open door or window, casts a strong beam of light down the center of the path. The light illuminates the floor, which appears to be made of concrete or asphalt, and creates a strong contrast with the surrounding darkness. The walls of the tunnel are also dark and textured.

Think Together.
Now.



Fallacy of Decentralisation:

*Between A and Z
or Liberating Dream?*

Nat Sakimura,
Chairman, OpenID Foundation
CEO, NAT.Consulting